(19)日本国特許庁（ＪＰ）　(12)特　許　公　報（Ｂ１）　(11)特許番号

第2884338号

(45)発行日　平成11年(1999)４月19日　(24)登録日　平成11年(1999)２月12日

(51)Int.Cl.[6]	識別記号	FI	
H04L 9/32			
G06F 12/14	320	H04L 9/00	675D
15/00	330	G06F 12/14	320C
		15/00	330B
		H04L 9/00	673D

発明の数２（全 14 頁）

(21)出願番号　特願平9－264850
(62)分割の表示　特願平8－56966の分割
(22)出願日　昭和59年(1984)10月11日

審査請求日　平成９年(1997)10月13日

許権者において、権利譲渡または実施許諾の用意がある。

早期審査対象出願

(73)特許権者　593187342
塚本　豊
奈良県吉野郡大淀町大字北野40番地の15
(72)発明者　塚本　豊
岡山県玉野市玉４丁目８番20号

審査官　徳永　民雄

(56)参考文献　特開　昭52－59540（ＪＰ，Ａ）
特開　昭57－111760（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.[6]，ＤＢ名)
H04L 9/00 － 9/38
H04K 1/00 － 3/00
G09C 1/00 － 5/00
G06F 15/00
G06F 12/00

(54)【発明の名称】　アクセス制御システム

1

(57)【特許請求の範囲】

1．アクセス希望者側が生成したパスワードデータに基づいて認証を行ないアクセス制御を行なうためのアクセス制御システムであって、
前記アクセス希望者がアクセスしようとする対象であって複数箇所に分散配置された複数のアクセス対象と、
該複数のアクセス対象それぞれについてアクセス要求があった場合のアクセス制御のための認証を統括して行なって集中管理を行なう認証手段と、
演算処理機能を有して前記アクセス希望者側においてパスワードデータを生成する手段であって、前記アクセス希望者側と前記認証手段側とでアクセス毎に共通に変化可能な共通変化データを利用してアクセス毎に内容が変化可能な可変型パスワードデータを演算して生成する可変型パスワードデータ生成手段とを含み、

2

前記アクセス希望者側が前記複数のアクセス対象のいずれかにアクセスするべく前記可変型パスワードデータを伝送した場合に該可変型パスワードデータが前記認証手段に転送され、
前記可変型パスワードデータ生成手段は、クロック機能を有し、該クロック機能が計時する時間に応じて変化する時間変数データを前記共通変化データとして利用して前記可変型パスワードデータを生成し、
前記認証手段は、時間に応じて変化する時間変数データを前記共通変化データとして用いて前記転送されてきた可変型パスワードデータの適否を判定して認証を行なう時間同期式認証手段を含み、
前記アクセス制御システムは、
前記可変型パスワードデータ生成手段のクロックが狂って前記時間変数データに誤差が生じた場合にその誤差を

自動的に修復させて経時的に誤差が累積されることを防止可能とするための誤差自動修復手段をさらに含み、
前記アクセス希望者は、前記認証手段により適正である旨の認証結果が得られたことを条件として前記アクセス対象へのアクセスが許容されることを特徴とする、アクセス制御システム。

2．アクセス希望者側が生成したパスワードデータに基づいて認証を行ないアクセス制御を行なうためのアクセス制御システムであって、
前記アクセス希望者がアクセスしようとする対象であって複数箇所に分散配置された複数のアクセス対象と、
該複数のアクセス対象それぞれについてアクセス要求があった場合のアクセス制御のための認証を統括して行なって集中管理を行なう認証手段と、
演算処理機能を有して前記アクセス希望者側においてパスワードデータを生成する手段であって、前記アクセス希望者側と前記認証手段側とでアクセス毎に共通に変化可能な共通変化データを利用してアクセス毎に内容が変化可能な可変型パスワードデータを演算して生成する可変型パスワードデータ生成手段とを含み、
前記アクセス希望者側が前記複数のアクセス対象のいずれかにアクセスするべく前記可変型パスワードデータを伝送した場合に該可変型パスワードデータが前記認証手段に転送され、
前記可変型パスワードデータ生成手段は、クロック機能を有し、該クロック機能が計時する時間に応じて変化する時間変数データを前記共通変化データとして利用して前記可変型パスワードデータを生成し、
前記認証手段は、時間に応じて変化する時間変数データを前記共通変化データとして利用して前記転送されてきた可変型パスワードデータの適否を判定して認証を行なう時間同期式認証手段を含み、
前記時間同期式認証手段は、
前記転送されてきた可変型パスワードデータが誤差を有する時間変数データにより生成されたものであっても、当該誤差が予め定められた誤差許容時間の範囲内のものである場合には当該誤差に起因したアクセス禁止の認証を行なわない所定誤差許容認証手段と、
前回のアクセス時から前記誤差許容時間の範囲内において、前回のアクセス時に用いられた可変型パスワードデータと同じ可変型パスワードデータによりアクセスをしてきた場合に、当該アクセスを許容しない旨の認定を行なうための誤差許容時間内不正アクセス禁止手段とを含むことを特徴とする、アクセス制御システム。

3．前記可変型パスワードデータ生成手段は、当該可変型パスワードデータ生成手段を所有している本人を確認するための識別データ信号が入力されたことを判別する識別信号入力判別手段を含み、該識別信号入力判別手段による入力判別が行なわれたことを条件として前記可変型パスワードデータの生成が可能となることを特徴とする、請求項1または請求項2に記載のアクセス制御システム。

4．前記認証手段が前記可変型パスワードデータに基づいたパスワード認証動作を行なう前に、前記アクセス希望者から通知された確認用データであって当該アクセス希望者が予め登録されているものか否かを確認するための登録確認用データに基づいて適正である旨の確認結果が得られたことを条件として、前記認証手段が前記パスワード認証動作を実行することを特徴とする、請求項1または請求項2に記載のアクセス制御システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、主として、あるアクセス対象設備へのアクセスを限られた者にのみ限定するべく、アクセス対象設備へのアクセスが許されるべきものか否かを認証してアクセス制御を行なうアクセス制御システムであり、詳しくは、アクセス希望者側がパスワードデータをデータ通信により伝送し、その伝送されてきたパスワードデータに基づいてアクセス制御を行なうアクセス制御システムに関する。

【０００２】

【従来の技術】この種のアクセス制御システムにおいて、従来から一般的に知られているものに、たとえば、特開昭５９－１０６８０号公報に記載のものがあった。この従来技術のものは、アクセス対象設備に一定のシークレットルール（パスワードデータの適否を判定する判定用データ）を前もって登録しておき、アクセス対象設備側で生成された乱数がアクセス希望者所有のパスワードデータ生成装置に入力されてその乱数を用いて生成されたパスワードデータが前記アクセス対象設備側に伝送され、前記アクセス対象設備側で前記登録されていたシークレットルールを用いて生成されたパスワードデータと伝送されてきたパスワードとが一致する場合にのみ、アクセス希望者が適正である旨の判別を行なってアクセス対象設備へのアクセスを許容するように構成されていた。つまり、前記乱数により、アクセス毎に変化可能なデータであってアクセス希望者側とアクセス対象設備側とで共通に変化可能な共通変化データが構成されており、この共通変化データを利用して毎回変化可能なパスワードデータを生成してアクセス許否の認証を行なっていた。

【０００３】ところが、高度情報化社会となり、この種のアクセス制御システムが普及した場合には、たとえば、コインロッカーのドアの解錠、自己の銀行口座の呼出し、使用者が限定されているシークレットな技術情報のファイル装置等からの呼出し等、本システムの使用頻度が増大し、多くのアクセス対象設備へのアクセスに使用されることになる。その結果、ユーザが利用しようとする多くのアクセス対象設備すべてに逐一前記シークレットルール等の判定用データを登録しておかなければな

らず、それだけ登録された判定用データの他人による盗用の機会が増大し、悪用による多大な損害が発生するという欠点が生ずる。特に高度情報化社会においては、個人のプライバシーや企業秘密の漏洩は万が一にもあってはならないのであり、前述した判定用データの盗用は厳に防止しなければならない。

【０００４】

【発明が解決しようとする課題】そこで、アクセス対象設備毎に異なった判定用データを登録し、たとえばそのうちの１つの判定用データが盗まれたとしても、他のアクセス対象設備へのアクセスに悪用されないようにする方法も考えられる。しかし、アクセス対象設備毎に使用対象となる判定用データをユーザが記憶または所有しておかなければならず、煩雑であり、特に、アクセス対象設備が多くなれば忘れる可能性もあり、不都合である。

【０００５】また、仮りに、前記登録された判定用データの盗用を完全に防止できたとしても、多くのアクセス対象設備すべてに逐一前記判定用データを登録するという従来技術の場合には、多くのアクセス対象設備に逐一判定用データを登録するという煩雑な作業が必要となるばかりでなく、たとえば前記パスワードデータ生成装置が盗難される等の原因で前記判定用データを新たなものに更新しなければならなくなった場合には、多くのアクセス対象設備すべてに登録されている判定用データを逐一すべて更新し直さなければならず、非常に煩雑な作業が強いられるという欠点が生ずる。本発明は、係る実情に鑑み考え出されたものであり、その目的は、アクセス対象か多くなったとしても、その多くのアクセス対象毎に判定用データの登録を行なう必要性をなくして、アクセス対象毎に判定用データの登録を行なうことによる前述した種々の不都合を防止できるアクセス制御システムを提供することである。

【０００６】

【課題を解決するための手段】本第１発明は、アクセス希望者側が生成したパスワードデータに基づいて認証を行ないアクセス制御を行なうためのアクセス制御システムであって、前記アクセス希望者がアクセスしようとする対象であって複数箇所に分散配置された複数のアクセス対象と、該複数のアクセス対象それぞれについてアクセス要求があった場合のアクセス制御のための認証を統括して行なって集中管理を行なう認証手段と、演算処理機能を有して前記アクセス希望者側においてパスワードデータを生成する手段であって、前記アクセス希望者側と前記認証手段側とでアクセス毎に共通に変化可能な共通変化データを利用してアクセス毎に内容が変化可能な可変型パスワードデータを演算して生成する可変型パスワードデータ生成手段とを含み、前記アクセス希望者側が前記複数のアクセス対象のいずれかにアクセスするべく前記可変型パスワードデータを伝送した場合に該可変型パスワードデータが前記認証手段に転送され、前記可変型パスワードデータ生成手段は、クロック機能を有し、該クロック機能が計時する時間に応じて変化する時間変数データを前記共通変化データとして利用して前記可変型パスワードデータを生成し、前記認証手段は、時間に応じて変化する時間変数データを前記共通変化データとして用いて前記転送されてきた可変型パスワードデータの適否を判定して認証を行なう時間同期式認証手段を含み、前記アクセス制御システムは、前記可変型パスワードデータ生成手段のクロックが狂って前記時間変数データに誤差が生じた場合にその誤差を自動的に修復させて経時的に誤差が累積されることを防止可能とするための誤差自動修復手段をさらに含み、前記アクセス希望者は、前記認証手段により適正である旨の認証結果が得られたことを条件として前記アクセス対象へのアクセスが許容されることを特徴とする。本第２発明は、アクセス希望者側が生成したパスワードデータに基づいて認証を行ないアクセス制御を行なうためのアクセス制御システムであって、前記アクセス希望者がアクセスしようとする対象であって複数箇所に分散配置された複数のアクセス対象と、該複数のアクセス対象それぞれについてアクセス要求があった場合のアクセス制御のための認証を統括して行なって集中管理を行なう認証手段と、演算処理機能を有して前記アクセス希望者側においてパスワードデータを生成する手段であって、前記アクセス希望者側と前記認証手段側とでアクセス毎に共通に変化可能な共通変化データを利用してアクセス毎に内容が変化可能な可変型パスワードデータを演算して生成する可変型パスワードデータ生成手段とを含み、前記アクセス希望者側が前記複数のアクセス対象のいずれかにアクセスするべく前記可変型パスワードデータを伝送した場合に該可変型パスワードデータが前記認証手段に転送され、前記可変型パスワードデータ生成手段は、クロック機能を有し、該クロック機能が計時する時間に応じて変化する時間変数データを前記共通変化データとして利用して前記可変型パスワードデータを生成し、前記認証手段は、時間に応じて変化する時間変数データを前記共通変化データとして利用して前記転送されてきた可変型パスワードデータの適否を判定して認証を行なう時間同期式認証手段を含み、前記時間同期式認証手段は、前記転送されてきた可変型パスワードデータが誤差を有する時間変数データにより生成されたものであっても、当該誤差が予め定められた誤差許容時間の範囲内のものである場合には当該誤差に起因したアクセス禁止の認証を行なわない所定誤差許容認証手段と、前回のアクセス時から前記誤差許容時間の範囲内において、前回のアクセス時に用いられた可変型パスワードデータと同じ可変型パスワードデータによりアクセスをしてきた場合に、当該アクセスを許容しない旨の認定を行なうための誤差許容時間内不正アクセス禁止手段とを含むことを特徴とする。

【０００７】

7

【作用】本第１発明によれば、複数箇所に分散配置された複数のアクセス対象に対し統括して認証を行なう認証手段が設置されており、その認証手段により、前記複数のアクセス対象それぞれについてアクセス要求があった場合のアクセス制御のための認証が統括して行なわれて集中管理が行なわれる。演算処理機能を有して前記アクセス希望者側においてパスワードデータを生成する可変型パスワードデータ生成手段の働きにより、前記アクセス希望者側と前記認証手段側とでアクセス毎に共通に変化可能な共通変化データを利用してアクセス毎に内容が変化可能な可変型パスワードデータが演算されて生成される。そして、前記アクセス希望者側が前記複数のアクセス対象のいずれかにアクセスするべく前記可変型パスワードデータを転送した場合にその可変型パスワードデータが前記認証手段に転送される。前記可変型パスワードデータ生成手段は、クロック機能を有しており、そのクロック機能が計時する時間に応じて変化する時間変数データを前記共通変化データとして利用して前記可変型パスワードデータが生成される。認証手段は、時間に応じて変化する時間変数データを前記共通変化データとして用いて前記転送されてきた可変型パスワードデータの適否を判定して認証を行なう時間同期式認証手段を含んでいる。そして、誤差自動修復手段の働きにより、可変型パスワードデータ生成手段のクロックが狂って前記時間変数データに誤差が生じた場合にその誤差を自動的に修復させて経時的に誤差が累積されることが防止可能となる。そして、アクセス希望者は、認証手段により適正である旨の認証結果が得られたことを条件としてアクセス対象へのアクセスが許容される。本第２発明によれば、複数箇所に分散配置された複数のアクセス対象に対し統括して認証を行なう認証手段が設置されており、その認証手段により、前記複数のアクセス対象それぞれについてアクセス要求があった場合のアクセス制御のための認証が統括して行なわれて集中管理が行なわれる。演算処理機能を有して前記アクセス希望者側においてパスワードデータを生成する可変型パスワードデータ生成手段の働きにより、前記アクセス希望者側と前記認証手段側とでアクセス毎に共通に変化可能な共通変化データを利用してアクセス毎に内容が変化可能な可変型パスワードデータが演算されて生成される。そして、前記アクセス希望者側が前記複数のアクセス対象のいずれかにアクセスするべく前記可変型パスワードデータを転送した場合にその可変型パスワードデータが前記認証手段に転送される。前記可変型パスワードデータ生成手段は、クロック機能を有しており、そのクロック機能が計時する時間に応じて変化する時間変数データを前記共通変化データとして利用して前記可変型パスワードデータが生成される。認証手段は、時間に応じて変化する時間変数データを前記共通変化データとして用いて前記転送されてきた可変型パスワードデータの適否を判定して認証を行なう時間同期式認証手段を含んでいる。そして、所定誤差許容認証手段の働きにより、前記転送されてきた可変型パスワードデータが誤差を有する時間変数データにより生成されたものであっても、当該誤差が予め定められた誤差許容時間の範囲内のものである場合には当該誤差に起因したアクセス禁止の認証が行なわれない。また、誤差許容時間内不正アクセス禁止手段の働きにより、前回のアクセス時から前記誤差許容時間の範囲内において、前回のアクセス時に用いられた可変型パスワードデータと同じ可変型パスワードデータによりアクセスをしてきた場合に、当該アクセスを許容しない旨の認定が行なわれる。

8

【０００８】

【発明の実施の形態】本発明に係るアクセス制御システムの実施の形態を説明する前に、高度情報化社会におけるデータ通信では必要性が高まるデジタル著名システムの実施の形態について説明する。

【０００９】図１に示すように、文字用キーと数字用キーにより平仮名と数字をインプットできるキーボード１を有するデータ入力手段の一例のデータ入力装置２に対し、ＲＡＭやＣＰＵ内蔵のパーソナル端末装置３を着脱自在に構成している。このパーソナル端末装置はディジタル署名をせんとするデータの送信者が個人的に所有する装置であればどのようなものであってもよく、従来から一般的に周知なものとしては、たとえばＩＣカード等が考えられる。

【００１０】この個人所有のパーソナル端末装置３の回路構成を図１０に示す。パーソナル端末装置３内には、ＣＰＵ５０と、ＲＯＭ５１と、ＲＡＭ５２と、Ｉ／Ｏポート５３とが設けられている。ＲＯＭ５１は、ＣＰＵ５０の動作プログラムすなわち後述する図２に示すフローチャートのプログラム等が記憶されている。ＣＰＵ５０は、そのＲＯＭ５１に記憶されているプログラムに従って動作し、後述する秘密ルールの一例の文字数字変換ルールやシークレット関数を呼出してＲＡＭ５２に記憶させる。そして、後述するように、キーボード１から入力されてＩ／Ｏポート５３から入力された送信データを、ＲＡＭ５２に記憶されている秘密ルールに従ったアルゴリズムにより、図２に示すように変換し、その変換データをＩ／Ｏポート５３から出力する。

【００１１】このパーソナル端末装置３に記憶されている秘密ルールは、平仮名文字を一定のルールに従って数字に変換するための文字数字変換ルールと、三角関数，指数関数等の組合せからなるシークレット関数ｆ（ｘ）等から構成されている。この秘密ルールはパーソナル端末装置３においてそれぞれ相違した種類のものが記憶され、そのため、署名せんとする各署名者がそれぞれこのパーソナル端末装置３を所有することによって、各署名者はそれぞれ自己固有の秘密ルールを保有することになる。また、この秘密ルールは対外的に秘密なものであ

る。

【００１２】そして、前記パーソナル端末装置３には、図２に示すフローチャートのプログラムが組込まれており、ディジタル署名を行なう場合には、前記パーソナル端末装置３を入力装置２に装着した状態で署名対象である契約書の文字等の送信データを平仮名の形でキーボード１から入力する。また、日付等の数字はそのまま入力する。そして、入力されたものが文字である場合には、前記文字数字変換ルールに従って入力毎に逐一文字を数字に変換して足し合わせ、さらに、入力されたものが数字である場合には、その数字をそのままの形で足し合わせ、次にＥＮＤ用キーＥのＯＮ操作があれば、すべての文字，数字の和Ｐ（ｎ）を前記シークレット関数ｆ（ｘ）に代入して答を算出し、その暗号化された符号からなる答である変換データ（この場合は数字となる）を署名データとしてＩ／Ｏポート５３から出力して表示部４に表示させる。そして、その表示部４に示された署名データを認証対象となる契約書等の送信データとともに送信する。

【００１３】前記入力装置２は、テレテックス端末機であってもよく、その場合には、署名対象物である送信データをテレテックス端末機のキーボードからパーソナル端末装置３に入力する。また、パーソナル端末装置３から出力された変換データである認証データを契約相手にテレテックス端末機から伝送するよう構成する。

【００１４】さらに、前記文字数字変換ルールとシークレット関数とからなる秘密ルールは、秘守義務のある官公庁等の公共機関やサービス機関等に登録しておく。

【００１５】書類受付印，受理印，金銭領収印のように、チェックのための認証を行なうディジタル署名の場合には、書類受付行為等の認証対象行為自体を平仮名文字でキーボード１から入力し、さらに、認証対象行為を行なった日付を入力して変換データすなわち署名データを算出する。たとえば、認証対象行為が書類受付であり、認証日付が１９８４年１０月９日１１時３５分であれば、キーボード１に、「しょるいうけつけ１９８４ねん１０がつ９ひ１１じ３５ふん」と入力する。

【００１６】また、書類受付行為，受理行為等の種々の代表的チェック行為をキーボード１における１つの操作ボタンに割り付けることによってワンタッチで入力できるように構成してもよい。

【００１７】さらに、本発明でいう認証対象行為として挙げた書類受付行為，受理行為等は単なる例示であり、その他、注文書，納品書，領収書等への認証における注文行為，品物納入行為，金銭領収行為等、種々のチェック行為が含まれることは言うまでもない。

【００１８】次に、別の例を説明する。

①　シークレット関数によって算出された数字をそのまま署名データとする代わりに、その算出された数字の一部または全部を、一定のシークレットなルールに基づいて、平仮名，片仮名，漢字アルファベット等の文字や、図形，記号またはそれらの組合せまたはそれらと色彩との組合せに変換して署名データとして用いる。

【００１９】②　前記秘密ルールをパーソナル端末装置３に記憶させる代わりに、図３に示すように、企業等のファイル装置５に記憶させておく。その場合には、テレテックス端末機６と前記ファイル装置５とをコンピュータ７を介してＬＡＮ８等で接続し、公衆回線等を利用して他の企業との間で行なわれるペーパレス取引の署名者が、自己の秘密ルールを前記テレテックス端末機６からの操作で呼出し、前記コンピュータ７によって暗号化等の変換作業を行なう。前記秘密ルール呼出しの際には、後述する個体識別システムを利用して、署名者が呼出指定している秘密ルールが本当にその署名者のものであるか否かをコンピュータ７によりチェックし、署名者のものであることが確認できた段階で初めて呼出指定された秘密ルールへのアクセスを可能にする。

【００２０】なお、図中９はノードである。

③　秘密ルールを企業内のファイル装置５から呼出す代わりに、秘密ルールが登録されている公共機関やサービス機関等のファイル装置、または、自宅のファイル装置からデータ通信により自己の秘密ルールを呼出し、その呼出したファイル装置に接続されているコンピュータで暗号化等の変換作業を行なう。

【００２１】④　前記パーソナル端末装置３を、その装置所有者が所有する発信機（たとえば指輪型のもの）からの所定の信号（発信機それぞれによって相違する）を受信できなくなれば、暗号化等の変換機能が停止するように構成し、パーソナル端末装置３の紛失時における他人の悪用を防止できるようにする。

【００２２】⑤　暗号化等の変換方法として、図２に示したＰ（Ｎ）＝Ｐ（Ｎ－１）＋Ｄ（Ｎ）の代わりに、Ｐ（Ｎ）＝Ｐ（Ｎ－１）＋Ｎ・Ｄ（Ｎ）、Ｐ（Ｎ）＝Ｐ（Ｎ－１）＋Ｄ（Ｎ）／Ｎ、Ｐ（Ｎ）＝Ｐ（Ｎ－１）／Ｎ＋Ｄ（Ｎ）、あるいは、Ｐ（Ｎ）＝Ｐ（Ｎ－１）／Ｎ＋Ｎ・Ｄ（Ｎ）等を用いる。

【００２３】次に、本発明に係るアクセス制御システム（個体識別システム）の実施の形態について説明する。このアクセス制御システムは、たとえば、前述したように、秘密ルール読出の際に読出指定された秘密ルールが本当に本人のものであるか否かを判別する等の場合にも利用できる。

【００２４】図４に示すように、銀行１０内の自己の口座の呼出し、データバンク１１内のシークレットな技術情報の検索、コインロッカ１２の解錠等、一定の限られたものにのみアクセスを許容するべき設備と、設備利用者（アクセス希望者）にアクセスを許容してもよいか否かの個体識別を判断する自宅または所定の機関のコンピュータ１３または１４とを公衆回線１５で接続し、それら設備１０，１１，１２と個体識別を行なうコンピュー

タ１３，１４との間でデータ通信が可能になるように構成している。また図中１６は網制御装置（ＮＣＵ）、１７は交換機である。

【００２５】そして、たとえば、データバンク１１内の技術情報を利用したい場合には、まず、キャプテン用端末機１８により、データバンク１１を呼出して所望の技術情報を検索してもらい、その技術情報が或る一定のものにしか使用許可されないシークレットな技術情報である場合には、以下の手順で個体識別を行なう。

【００２６】①　技術情報を使用せんとする設備利用者が個体識別を行なう自宅または所定機関のコンピュータ１３または１４の呼出番号をデータバンク１１に知らせる。

【００２７】②　データバンク１１側は、その番号が前もって登録されている使用許可できるものの番号であるか否かを確認し、使用許可者の番号であれば識別信号の送信を要求し、使用許可者の番号でなければ使用を許可しない。

【００２８】③　前記識別信号の送信要求がでれば設備利用者は自己所有の装置３３からアウトプットされた識別信号をキャプテン用端末機１８によりデータバンク１１側に送信する。

【００２９】④　データバンク１１側は送信されてきた識別信号を前記呼出番号のコンピュータ１３または１４に送信し、そのコンピュータ１３または１４で送信されてきた識別信号が正しいものか否かの個体識別判断（後述する）を行ない、その結果をデータバンク１１側に送信する。

【００３０】⑤　データバンク１１側では、正しいという判断結果が送信されてきた場合にのみ呼出指定されているシークレット技術情報へのアクセスを許可する。

【００３１】次に、コインロッカ１２を解錠する場合の手順は、まず、解錠状態にあるコインロッカのドア内面側にあるキーボードの操作によって個体識別を行なう自宅または所定機関のコンピュータ１３または１４の呼出番号をインプットし、予め前記コンピュータ１３または１４を登録し解錠操作時に自動的にそのコンピュータ１３または１４が呼出されるように設定した状態でドアを閉じて錠をかけ、解錠時には、そのコインロッカのドア外面から識別信号をインプットし、前述した④，⑤と同様の方法により解錠制御を行なう。

【００３２】次に、たとえば、金銭の支払いに際して、自己の銀行口座の預金を金銭受取人の銀行口座内に移動させるという数字の移動のみで現金の移動を伴わないキャッシャレス支払システム（銀行ＰＯＳシステム）等において、自己の銀行口座を呼出す手順は、まず、銀行に前もって自宅または所定機関のコンピュータ１３または１４の呼出番号を登録しておき、自己の銀行口座の呼出指定があった場合には、自動的に前記コンピュータ１３または１４が呼出されるように設定しておく。そして、

スーパマーケット等で物を購入して支払いをする場合には、そのスーパマーケット等のレジスタ１９から自己の銀行口座の呼出指定を行ない、前記④，⑤と同様の方法で自己の銀行口座へのアクセスを行なう。なお、自己の銀行口座呼出指定手段としては、設備利用者所有の装置３３から出力された銀行口座呼出指定信号をレジスタ１９から入力し、銀行へ伝送する方法を用いる。

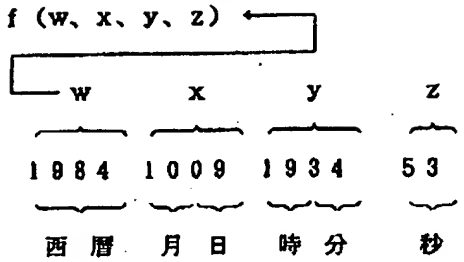
【００３３】また、自動車等のドアの解錠、エンジンの始動等のアクセスは利用対象設備が移動物であるために、公衆回線等の有線系メディアによるデータ通信は不可能であり、衛星通信等の無線系メディアを用いる。このように、本発明でいう「データ通信」とは、有線系メディアばかりでなく無線系メディアをも含む広い概念である。

【００３４】次に、前述した個体識別方法を説明する。図５に示すように、ＪＪＹによる時刻標準電波等のコード／データ放送を受信し、その受信信号に基づいて時刻を表示する腕時計により設備利用者所有の装置３３を構成してある。そして、腕時計３３内に記憶されているシークレットルールとしてのシークレット関数（それぞれの腕時計によって相違する）に、その腕時計３３が表示している現在の時刻を入力信号として代入し、答えを算出し、その答えと使用した入力信号のうち秒に相当する部分を識別信号としてアウトプットする。アウトプットの方法は、図６に示すように、まず送信ボタン２１を押し、腕時計裏面の伝導板からなる信号送出し部２２から手２３にパルス電流として識別信号が一定時間（１０秒間）送り出され、導体である手２３を媒体として、レジスタ１９、コインロッカ１２、自動車２０、キャプテン用端末機１８、電話機、テレテックス用端末機等の識別信号受信部２４へ送信される。送信された識別信号は、個体識別判断を行なう自宅または所定の機関のコンピュータ１３または１４へ送られ、そのコンピュータに予め登録されているシークレットルールとしてのシークレット関数に入力信号を代入して答えを算出し、その答えと識別信号とを比較して正しいか否かを判断し、個体識別を行なう。

【００３５】前記シークレット関数は、三角関数、指数関数等の組合せからなる関数で、４つの変数ｗ、ｘ、ｙ、ｚを有し、以下に示す数１のように、入力信号のそれぞれの部分をｗ、ｘ、ｙ、ｚに代入して答えを算出する。

【００３６】

【数１】



【００３７】また、外国から我が国へ識別信号を送る場合には、外国の時刻を我が国の時刻に変換した入力信号をシークレット関数に代入する必要がある。

【００３８】図中２５は或る一定の信号を発生する設備利用者所有の指輪型発信機であり、発信機それぞれによって発信信号が相違するもので、前記腕時計３３が、その発信機２５からの所定の信号を受信しているときにのみ識別信号を発信するように構成し、腕時計３３紛失時における他人の悪用を防止する。

【００３９】図中２６は、自己の銀行口座呼出しの際等に使用するキーボードであり、暗証番号をインプットしたり、銀行口座呼出指定信号をアウトプットさせたりするもので、それら信号は、識別信号と同様に信号送出し部２２からアウトプットされる。

【００４０】なお、前記腕時計３３は、コード／データ放送による信号に基づいて逐一表示時刻との誤差が修正されるように構成されているものであり、腕時計３３内に組込まれるプログラムのフローチャートを図７に示す。ゆえに、この腕時計３３は、プログラムに従って動作するマイクロコンピュータすなわち図１０に示す回路構成と同様のものが内蔵されている。

【００４１】図７に示すフローチャートを簡単に説明する。ステップＳ（以下単にＳという）１により、コード／データ放送による時刻標準電波を受信したか否か判別され、受信するまで待機する。そして受信した場合にはＳ２に進み、その時刻標準電波に基づき分周器を修正し、修正後の時刻を表示する動作が行なわれる。次にＳ３に進み、受信機２５（図５参照）からの信号を受信しているか否かの判断がなされ、受信していない場合にはＳ１に戻るが、受信している場合にはＳ４に進み、個人識別信号の受信ボタン２１（図６参照）がＯＮ操作されたか否かの判断がなされ、操作されていない場合にはＳ１に戻るが、操作された場合にはＳ５に進み、シークレット関数ｆ（ｗ，ｘ，ｙ，ｚ）のそれぞれのｗ，ｘ，ｙ，ｚに現在の時刻からなる入力信号だ代入し、答えＡを算出する処理がなされる。次にＳ６に進み、その算出した答えＡとｚに代入された数値ＮＺとを識別信号としてアウトプットする処理がなされる。

【００４２】次に、シークレットルールが登録されているコンピュータ１３または１４に組込まれるプログラムのフローチャートを図８に示す。図８に基づいてこのフローチャートを簡単に説明する。Ｓ７において、識別信号ＡとＮＺとを受信したか否かの判断がなされ、受信するまで待機する。そして受信した段階でＳ８に進み、現在の時刻とＮＺとの差が許容値Ｋ秒以内であるか否かの判断がなされ、許容値Ｋ秒以内でなかった場合には、Ｓ１２に進み、設備へのアクセスは許容できないとの判断をアウトプットする処理がなされてＳ７に戻る。この許容値Ｋは、腕時計３３内で識別信号を算出するまでに要する時間やシークレットルール登録コンピュータ１３または１４までのデータ通信所要時間等を考慮した遅延時間であり、たとえば３秒等の短い時間である。

【００４３】そして、Ｓ８により許容値Ｋ秒以内であると判断された場合にはＳ９に進み、今回の識別信号受信時刻が前回の受信時刻から前記許容値Ｋ秒以上経過しているか否かの判断がなされ、経過していない場合にはＳ１２に進み、アクセスが許容できない旨の判断がなされる。このように、今回の識別信号受信時刻が前回の識別信号受信時刻から前記許容値Ｋ秒以上経過していることがアクセス許容条件に加えられている理由は、識別信号Ａと前記ＮＺが送信されたときから前記許容値Ｋ秒以内においてシステム悪用者が前記識別信号Ａと前記ＮＺとを記録してシークレットルール登録コンピュータ１３または１４に送信して不当に設備へのアクセスを行なう不都合を防止するためである。

【００４４】そしてこのＳ９により許容値Ｋ秒以上経過していると判断された場合にはＳ１０に進み、予め登録されているシークレット関数ｆ（ｗ，ｘ，ｙ，ｚ）のｗ，ｘ，ｙに現在の時刻からなる入力信号を代入し、ｚに前記ＮＺを代入して答えＢを算出する処理がなされる。そしてＳ１１に進み、そのＢと前記受信したＡとが等しいか否かの判断がなされ、等しくなければＳ１２に進み、アクセスを許容できない旨の判断がなされ、等しい場合にはＳ１３に進み、設備へのアクセスを許容できるとの判断をアウトプットする処理がなされてＳ７に戻る。

【００４５】次に、この固体識別システムの発明の別実施の形態を説明する。

（１）　前記シークレット関数への入力信号として、現在の時刻を用いる代わりに、コード／データ放送に基づいて経時的に増加または減少する全国共通または全世界共通の数字を用いる。その場合に、レジスタ１９、キャプテン用端末機１８等の識別信号入力端子から前記入力信号用数字を発信してもよく、設備利用者所有の装置３３への送信手段は、電波送信またはケーブルの接続のどちらでもよい。

【００４６】さらに、設備利用者所有の装置３３は腕時計に限らず、電子卓上計算機等の個人端末であれば何でもよい。

【００４７】（２）　入力信号として、未だに使用されたことのないものを用いる選択使用手段として、過去に

用いられたことのある入力信号を拒絶する機能をシークレットルール登録コンピュータ１３または１４に付加する。この場合のシークレットルール登録コンピュータ１３または１４に組込むプログラム、設備利用者所有の装置３３に組込むプログラムのそれぞれのフローチャートを図９（Ａ）、（Ｂ）に示す。

【００４８】この図９（Ａ）、（Ｂ）に示すフローチャートを簡単に説明する。まず図９（Ｂ）に基づいて設備利用者所有の装置３３に組込まれているプログラムを説明する。Ｓ２２において、Ｉの初期値が「１」に設定される。次にＳ２３に進み、送信ボタン２１（図６参照）がＯＮ操作されたか否かの判断がなされ、されるまで待機する。そして操作された段階でＳ２４に進み、シークレット関数ｆ（ｘ）に前記Ｉを代入し、ｆ（Ｉ）の値Ａを算出する処理がなされる。この段階では、前記Ｉは「１」となっている。次にＳ２５に進み、Ａ，Ｉそれぞれの値を識別信号としてアウトプットする処理がなされ、次にＳ２６に進み、現在のＩの値に「１」を加算して新たなＩの値とする処理がなされた後にＳ２３に戻る。

【００４９】このように、設備利用者所有の装置３３を利用して第１回目のアクセスを試みる場合には、前記ｆ（Ｉ）にＩ＝１が代入されて算出された識別信号Ａがシークレットルール登録コンピュータ１３または１４に伝送されることとなる。そして２回目のアクセスを試みる場合には、設備利用者所有の装置３３の送信ボタン２１がＯＮ操作されてＳ２４の識別信号Ａを算出する段階では、Ｉ＝２となっているために、ｆ（Ｉ）にＩ＝２が代入されて算出された識別信号Ａが伝送されることとなる。

【００５０】このように、装置３３では、送信ボタン２１がＯＮ送信されてアクセス動作が行なわれるたびにＩが「１」ずつ加算更新されるために、アクセス動作するたびに毎回異なったＩが用いられ、その結果毎回異なった識別信号Ａが算出されて伝送されることとなる。

【００５１】次にシークレットルール登録コンピュータ１３または１４に組込まれているプログラムを図９（Ａ）に基づいて説明する。Ｓ１４により、Ｊの初期値が「１」に設定され、次にＳ１５に進み、装置３３から伝送されてきた識別信号ＩとＡとを受信したか否かの判断がなされ、受信するまで待機する。そして受信した段階でＳ１６に進み、Ｊ＝Ｉであるか否かの判断がなされる。第１回目のアクセス動作時においては、Ｊが「１」となっており、Ｉも「１」となっているはずであるために、Ｓ１６によりＹＥＳの判断がなされるはずである。ところが、不正に設備へのアクセスを試みんとした者は、現時点でＩがいくらの値になっているか判別できないために、Ｉに適当な値を代入してコンピュータ１３または１４に伝送する場合が考えられる。その場合には、Ｓ１６によりＮＯの判断がなされてＳ１７に進み、設備

へのアクセスを許容できないとの判断をアウトプットする処理がなされてＳ１５に戻る。

【００５２】一方、Ｊ＝Ｉと判断された場合にはＳ１８に進み、登録されているシークレット関数ｆ（ｘ）にＪを代入して答えＢを算出する処理がなされる。次にＳ１９に進み、その算出したＢと前記伝送されてきたＡとが等しいか否かの判断がなされ、等しくない場合にはＳ１７に進み、設備へのアクセスを許容できない旨の判断がなされるが、等しい場合にはＳ２０に進み、設備へのアクセスを許容できるとの判断をアウトプットする処理がなされる。次にＳ２１に進み、現時点でのＪの値に「１」を加算してＪを更新する処理がなされた後Ｓ１５に戻る。

【００５３】このように、シークレットルール登録コンピュータ１３または１４は、装置３３から識別信号Ａ，Ｉが伝送されてくるたびにＪの値を「１」ずつ加算更新するのであり、その結果装置３３の現時点におけるＩの値とシークレットルール登録コンピュータ１３または１４の現時点におけるＪの値とは同期して同じ値となっているはずである。

【００５４】（３）　指名手配者等の操作対象人間のシークレットルールを登録し、そのシークレットルール登録コンピュータに識別信号が伝送されてきた場合には、その識別信号を入力した端末機に場所通達指令信号を返送し、その端末機から警察のコンピュータ等に端末機設置場所を表示する信号を伝送するように構成する。

【００５５】（４）　前記固体識別のために用いられたシークレットルールを前述のディジタル著名システムの発明に用いた秘密ルールによって肩代わりさせる。つまり、ある人物が所有する秘密ルールを、前記ディジタル著名システムと固体識別システムとに兼用使用する。

【００５６】次に、以上説明した種々の実施の形態の内容をまとめて以下に列挙する。

①　前記固体識別システム（アクセス制御システム）において、前記選択使用手段として、過去において使用されたことのある入力信号を拒絶する機能を前記判断手段側に持たせる。

【００５７】②　前記固体識別システムにおいて、前記選択使用手段として、全国共通でしかも選択使用毎にまたは経時的に増加または減少する数字を前記入力信号として用いる。

【００５８】③　前記②に記載した固体識別システムにおいて、前記数字が、コード／データ放送によって伝送されてきた信号に基づいて定められたものである。

【００５９】④　前記②または③に記載された固体識別システムにおいて、前記数字が、現在の年月日時刻を表わすものである。

【００６０】⑤　前記②に記載された固体識別システムにおいて、前記設備利用者の装置が腕時計で構成され、その腕時計が表示されている時刻を入力信号として使用

する。

【００６１】⑥　前記⑤に記載した固体識別システムにおいて、前記腕時計が、コード／データ放送によって伝送されてきた信号に基づいて時刻表示可能なものである。

【００６２】⑦　前記③または⑥に記載の固体識別システムにおいて、前記コード／データ放送が、利用対象となる個々の設備から発信されているものである。

【００６３】⑧　前記⑤または⑥に記載の固体識別システムにおいて、前記腕時計が、アウトプットされた識別信号を人間の手を媒体として利用対象設備側に伝送するべく、人間の手への信号送り出し部を有するものである。

【００６４】⑨　前記固体識別システムにおいて、前記設備利用者所有の装置が、その装置所有者が所有する発信機からの所定の信号を受信できなくなれば、固体識別のための機能が停止するもので構成されている。

【００６５】次に、本発明の構成要件と前記実施の形態との対応関係を説明する。前記シークレット関数ｆ（ｗ，ｘ，ｙ，ｚ）または図９に示したｆ（Ｉ），ｆ（ｘ）により、アクセス希望者固有の秘密の変換用データが構成されている。前記設備利用者所有の装置３３により、アクセス希望者固有の秘密の変換用データを記憶している、前記アクセス希望者所有のパーソナル演算装置が構成されている。そして、前述したように、図７のＳ５，図８のＳ１０に示された現在の時刻あるいは図９のＳ２４に示されたＩ，Ｓ１８に示されたＪにより、前記パーソナル演算装置と後述するアクセス許否判定手段との両者に共通に使用される変数データであって、前回のアクセス時と今回のアクセス時とで変化可能な変数データが構成されている。そして前記パーソナル演算装置は、前述したように、前記秘密の変換用データに従って所定のアルゴリズムにより前記選択された変数データを変換するための動作機能を有する。

【００６６】前記シークレットルール登録コンピュータ１３または１４により、アクセスを許容するか否かを判定するアクセス許否判定手段が構成されている。前記パーソナル演算装置が変換した変換済みデータ（Ａ等の識別信号）は、前述したように、前記データ通信（図４参照）により前記アクセス許否判定手段に伝送される。そしてアクセス許否判定手段は、前記伝送されてきた変換済みデータの適否を前記選択された変数データに基づいて判別する。

【００６７】前記銀行１０，データバンク１１またはコインロッカー１２により、アクセス希望者がアクセスしようとするアクセス対象が構成されている。コンピュータ１３または１４により、前記アクセス対象とは別の場所に設置されて該アクセス対象側とデータ通信が可能であり、アクセス制御のための認証を統括して行なって集中管理を行なう認証手段が構成されている。そして、前述したように、アクセス希望者側が前記アクセス対象側に前記パスワードデータを伝送した場合にはそのパスワードデータがデータ通信により前記認証手段に転送される。

【００６８】図８のＳ１０のシークレット関数ｆ（ｗ，ｘ，ｙ，ｚ）により、アクセス希望者側の前記パスワードデータの適否を判定するための判定用データが構成されている。そして前記認証手段は、前記アクセス希望者側の前記パスワードデータの適否を判定するための判定用データが格納されており、その判定用データを用いて前記転送されてきたパスワードデータの適否を判定して認証を行ない（図８のＳ１１）、その認証結果を前記パスワードデータの転送元であるアクセス対象側に返信する。

【００６９】そして前述したように、前記アクセス対象側は、適正である旨の認証結果が返信されてきたことを条件として当該アクセス希望者のアクセスを許容する。

【００７０】図７のＳ５の現在時刻からなる入力信号、または、図９（Ｂ）のＳ２４のＩにより、前記アクセス希望者側と前記認証手段側とで共通に変化可能なデータであってアクセス毎に変化可能な共通変化データが構成されている。図７のＳ５の答えＡまたは図９（Ｂ）のＳ２５のＡにより、前記共通変化データを利用してアクセス毎に内容が変化可能な可変型パスワードデータが構成されている。前記腕時計３３により、前記共通変化データを利用してアクセス毎に内容が変化可能な可変型パスワードデータを前記アクセス希望者側において生成する可変型パスワードデータ生成手段が構成されている。図８のＳ７により、前記可変型パスワードデータ生成手段により生成された可変型パスワードデータであってデータ通信により伝送されてきた可変型パスワードデータを受信するデータ受信手段が構成されている。図８のＳ８～Ｓ１１により、時間に応じて変化する時間変数データを前記共通変化データとして用いて前記データ受信手段で受信した可変型パスワードデータの適否を判定して認証を行なう時間同期式認証手段が構成されている。図８のＳ８により、前記データ受信手段により受信された前記可変型パスワードデータが誤差を有する時間変数データにより生成されたものであっても、当該誤差が予め定められた誤差許容時間（許容値Ｋ秒）の範囲内のものである場合には当該誤差に起因したアクセス禁止の認証を行なわない所定誤差許容認証手段が構成されている。図８のＳ９により、前回のアクセス時から前記誤差許容時間が経過するまでの間において、前回のアクセス時に用いられた可変型パスワードデータと同じ可変型パスワードデータによりアクセスしてきた場合に、当該アクセスを許容しない旨の認定を行なうための誤差許容時間内不正アクセス禁止手段が構成されている。図７のＳ１，Ｓ２により、前記の可変型パスワードデータ生成手段のクロック機能の狂いに伴い前記時間変数データに誤差が生

じた場合にそれを自動的に修復させて経時的に誤差が累積されることを防止するための誤差自動修復手段が構成されている。

【００７１】前述した図７のＳ３により、前記可変型パスワードデータ生成手段を所有している本人を確認するための識別データ信号が入力されたことを判別する識別信号入力判別手段が構成されている。そして、この識別信号入力判別手段による入力判別が行なわれたことを条件として前記可変型パスワードデータの生成が可能となる（図７のＳ３によりＹＥＳの判断がなされたことを条件としてＳ４～Ｓ６の処理が可能となる）。また、前述したように、認証手段が前記可変型パスワードデータに基づいたパスワード認証動作を行なう前に、前記アクセス希望者から通知された確認用データであって当該アクセス希望者が予め登録されているものか否かを確認するための登録確認用データ（呼出番号）に基づいて適正である旨の確認結果（呼出番号が前もって登録されている使用許可できるものの番号である旨の確認結果）が得られたことを条件として、前記認証手段が前記パスワード認証動作を実行する。

【発明の効果】本第１発明によれば、アクセス対象が多くなったとしても、アクセス制御のための認証を統括して行なって集中管理を行なう認証手段に認証用データを登録しておくことにより、前記複数のアクセス対象のうちのいずれかにアクセスするべくアクセス希望者が可変型パスワードデータを伝送した場合に、その可変型パスワードデータが前記認証手段に転送されてその認証手段において認証が行なわれるために、多くのアクセス対象毎に認証用データを登録する必要がなくなり、多くのアクセス対象毎に認証データを登録した場合の種々の不都合を極力防止することができる。さらに、時間に応じて変化する時間変数データを共通変化データとして用いて転送されてきた可変型パスワードデータの適否が判定されて認証が行なわれるために、前回のアクセス時と今回のアクセス時とで異なった内容の可変型パスワードデータとなり、セキュリティが向上する。しかも、可変型パスワードデータ生成手段のクロックが狂って時間変数データに誤差が生じた場合にその誤差が自動的に修復されて経時的に誤差が累積されることが防止可能となるために、時間変数データの誤差に起因したアクセス不能状態等が発生する不都合を極力防止することができる。本第２発明によれば、アクセス対象が多くなったとしても、アクセス制御のための認証を統括して行なって集中管理を行なう認証手段に認証用データを登録しておくことにより、前記複数のアクセス対象のうちのいずれかにアクセスするべくアクセス希望者が可変型パスワードデータを伝送した場合に、その可変型パスワードデータが前記認証手段に転送されてその認証手段において認証が行なわれるために、多くのアクセス対象毎に認証用データを登録する必要がなくなり、多くのアクセス対象毎に認証

データを登録した場合の種々の不都合を極力防止することができる。さらに、時間に応じて変化する時間変数データを共通変化データとして用いて転送されてきた可変型パスワードデータの適否が判定されて認証が行なわれるために、前回のアクセス時と今回のアクセス時とで異なった内容の可変型パスワードデータとなり、セキュリティが向上する。さらに、転送されてきた可変型パスワードデータが誤差を有する時間変数データにより生成されたものであっても、当該誤差が予め定められた誤差許容時間内の範囲内のものである場合に、当該誤差に起因したアクセス禁止の認証が行なわれないために、多少の誤差に起因してアクセス不能状態となる等の不都合を極力防止することができる。一方、誤差許容時間を設けた場合に、たとえば可変型パスワードデータが入力途中や伝送途中で盗聴されてその同じ可変型パスワードデータを用いて前記誤差許容時間の範囲内において不正にアクセスしようとする不正行為が発生することが考えられる。すなわち、前記誤差許容時間は、その時間内であれば誤差があってもアクセス禁止の認証を行なわないものであり、誤差許容時間内であれば結果として同じ内容の可変型パスワードデータを複数回受付けてしまい、この誤差許容時間がセキュリティホールとなってしまう虞れがある。そこで、本発明によれば、前回のアクセス時から前記誤差許容時間の範囲内において、前回のアクセス時に用いられた可変型パスワードデータと同じ可変型パスワードデータによりアクセスをしてきた場合に、当該アクセスを許容しない旨の認定を行なって誤差許容時間内における不正アクセスを禁止できるようにしたのであり、これによりより一層セキュリティが向上する。

【図面の簡単な説明】

【図１】斜視図である。

【図２】フローチャートである。

【図３】作用説明図である。

【図４】作用説明図である。

【図５】作用説明図である。

【図６】斜視図である。

【図７】フローチャートである。

【図８】フローチャートである。

【図９】（Ａ）（Ｂ）はそれぞれフローチャートである。

【図１０】パーソナル端末装置の制御回路図である。

【符号の説明】

３はパーソナル端末装置、２は入力装置、１はキーボード、３３は腕時計、１３，１４はコンピュータ、１０は銀行、１１はデータバンク、１２はコインロッカー、２５は発信機である。

【要約】

【課題】　アクセス対象設備が多くなったとしても、パスワードデータの適否を判定するための判定用データをそのアクセス対象設備ごとに登録する必要をなくし、登

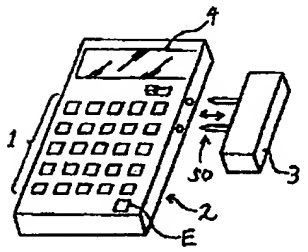
21

録された判定用データの盗用の危険性を極力抑える。

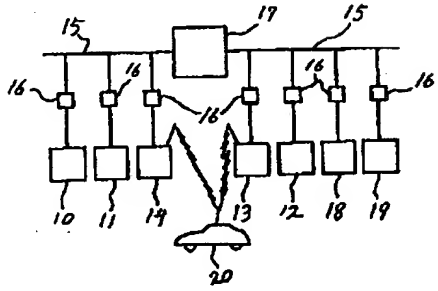
【解決手段】　アクセス希望者から送られてきたパスワードデータの適否を判定するための判定用データであるシークレット関数ｆ（ｗ，ｘ，ｙ，ｚ）をコンピュータ１３または１４に登録しておき、複数のアクセス対象設備１０，１１，１２のいずれにアクセスする場合においてもアクセス対象設備に伝送されてきたパスワードデータをコンピュータ１３または１４に転送し、そのコンピュータ１３または１４によってパスワードデータの適否を統括して判定して認証を行ない、その認証結果を転送元であるアクセス対象設備に返信するようにした。

22

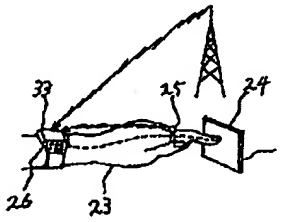
【図１】



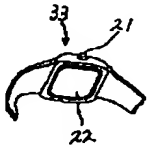
【図４】



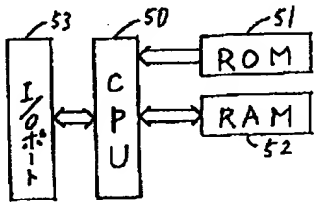
【図５】



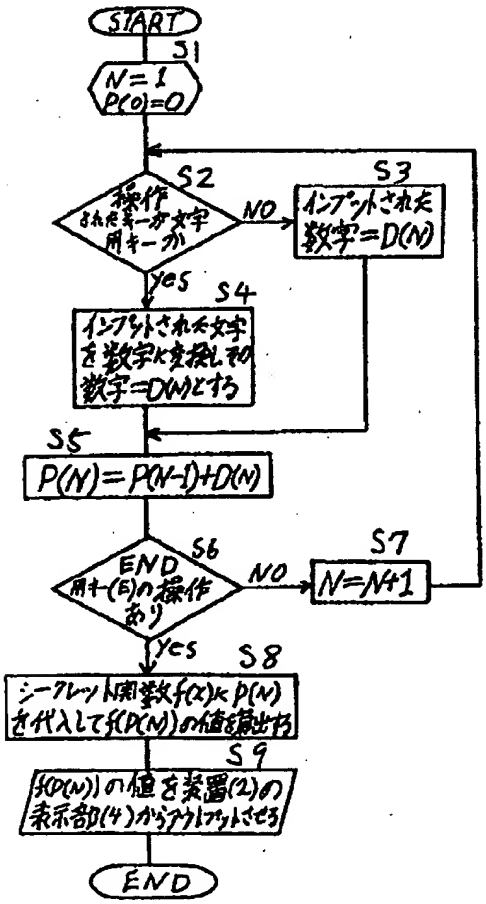
【図６】



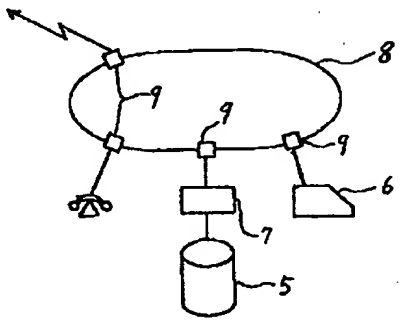
【図１０】



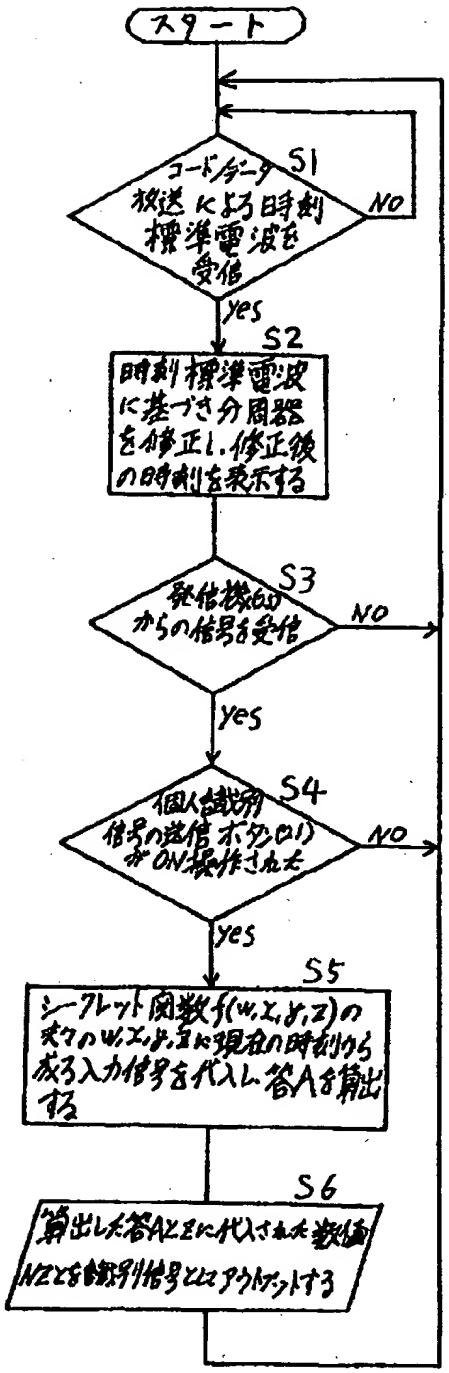
【図２】



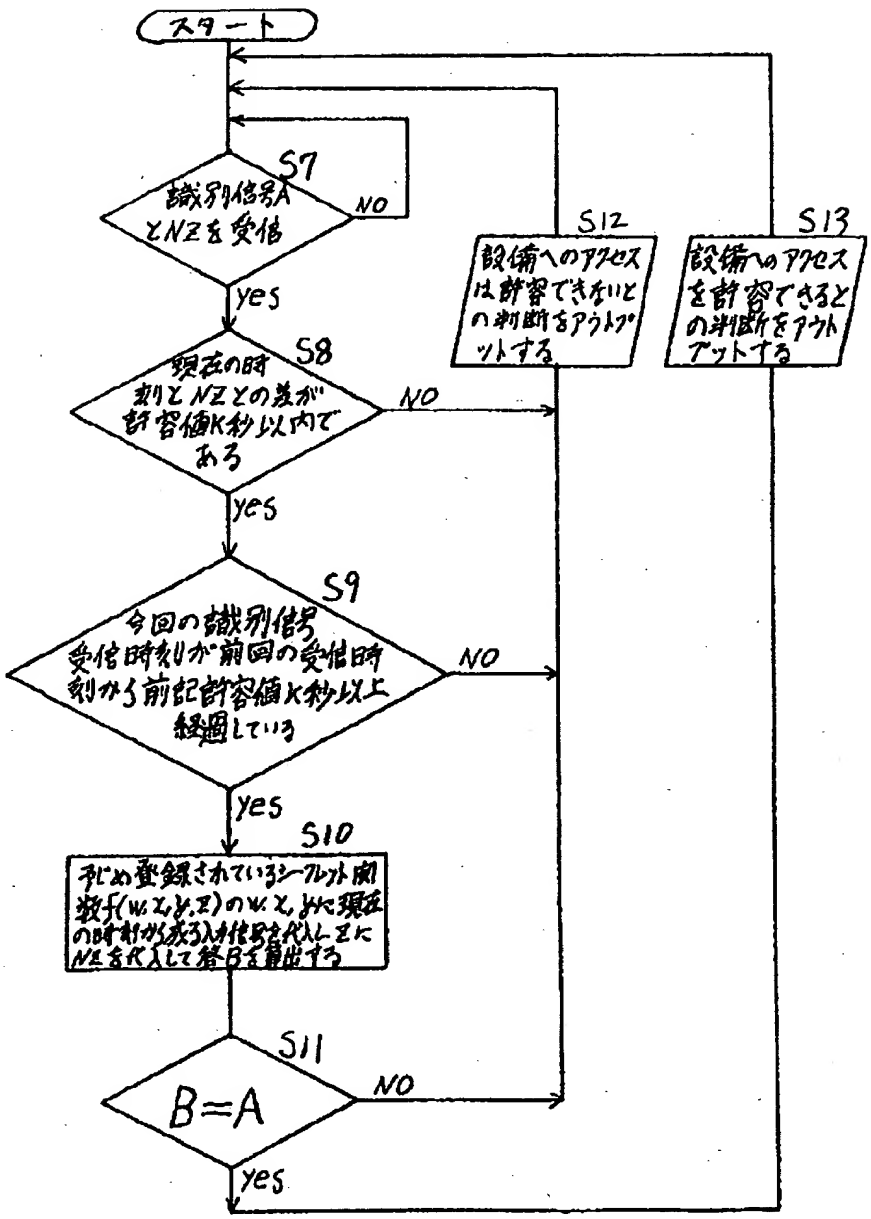
【図３】



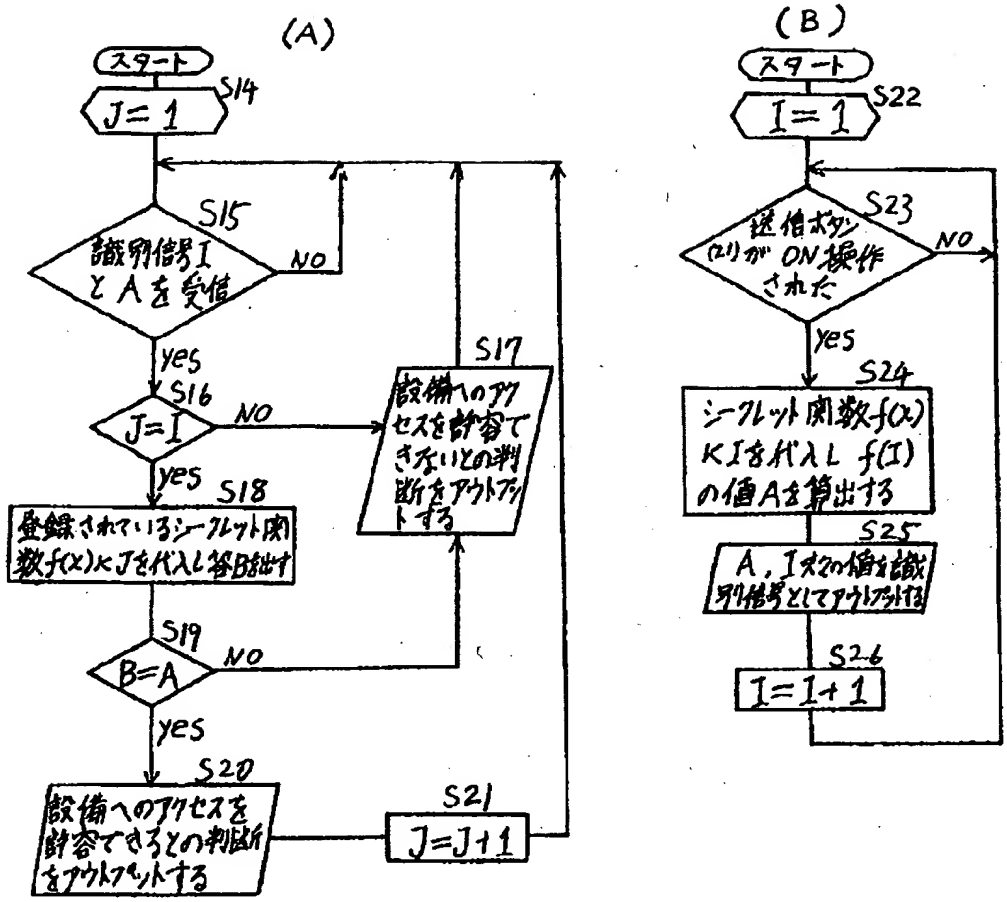
【図7】


スタート
S1
コードデータ
放送による日時刻
標準電波を
受信
NO
yes
S2
時刻標準電波に
基づき分周器
を修正し、修正後
の時刻を表示する
S3
発信機60
からの信号を受信
NO
yes
S4
個人識別
信号の送信ボタン(01)
がON操作された
NO
yes
S5
シークレット関数f(w,x,y,z)の
変数のw,x,y,zに現在の時刻から
成る入力信号を代入し、答Aを算出
する
S6
算出した答AとZに代入された数値
NZとを識別信号としてアウトプットする

【図８】


スタート
S7
識別信号AとNZを受信
NO
yes
S8
現在の時刻とNZとの差が許容値K秒以内である
NO
yes
S9
今回の識別信号受信時刻が前回の受信時刻から前記許容値K秒以上経過している
NO
yes
S10
予じめ登録されているシークレット関数f(w,x,y,z)のw,x,yに現在の時刻から成る入力信号を代入しzにNZを代入して答Bを算出する
S11
B=A
NO
yes
S12
設備へのアクセスは許容できないとの判断をアウトプットする
S13
設備へのアクセスを許容できるとの判断をアウトプットする

【図９】


(A)
スタート
S14
J=1
S15
識別信号I
とAを受信
NO
yes
S16
J=I
NO
S17
設備へのアクセスを許容できないとの判断をアウトプットする
yes
S18
登録されているシークレット関数f(x)にJを代入し答Bを出す
S19
B=A
NO
yes
S20
設備へのアクセスを許容できるとの判断をアウトプットする
S21
J=J+1
(B)
スタート
S22
I=1
S23
送信ボタン(21)がON操作された
NO
yes
S24
シークレット関数f(x)にIを代入しf(I)の値Aを算出する
S25
A,Iその値を識別信号としてアウトプットする
S26
I=I+1